DEPARTMENT OF THE TREASURY
WASHINGTON

INSPECTOR GENERAL

December 30, 1998

MEMORANDUM FOR PHILIP DIEHL, DIRECTOR
UNITED STATES MINT

FROM: David C. Williams
Inspector General David C. Williams

SUBJECT: Year 2000 Compliance Effort at the United States Mint

This memorandum presents the results of our assessment of the United States Mint's (Mint) Year 2000 conversion effort. We performed a limited review of this effort. In addition to the Mint, the Office of Inspector General (OIG) evaluated and reported on the Year 2000 efforts at other Treasury bureaus individually, as well as from a Department-wide perspective. Subsequent work may be performed by us in the future and will be reported to you in a separate report.

Overall, we concluded that the Mint established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. No significant reportable issues came to our attention. However, the inherent nature of the Year 2000 dilemma denies the ability to completely eliminate risk. The Year 2000 problem comes with inherent risks that all organizations face and will continue to face, despite their best efforts and demonstrated success. Accordingly, we have developed three suggestions encouraging organizations to sustain their efforts in the areas of change management, data exchange, and contingency planning for business continuity to minimize potential disruptions caused by these inherent risks.

Although an official written response was not required because we made no recommendations for corrective action, the Mint provided their comments to our draft report. The Mint concurred with the OIG findings and suggestions, and the full text of their response is included as Appendix 1.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objective of our review was to evaluate the Mint's internal Year 2000 conversion effort for its mission critical information technology (IT) systems. Our specific objectives were to evaluate the following: (1) project management; (2) system conversion and certification; and (3) contingency planning for business continuity. In addition, we performed a limited review of the Mint's Year 2000 strategy and progress for non-IT and telecommunications systems.

Our review was limited to evaluating strengths and weaknesses in the management of the Year 2000 conversion project. Specifically, we determined if processes existed and were designed to mitigate the Year 2000 risk to an acceptable level for ensuring all mission critical IT systems remain operable. Therefore, this memorandum is not intended to represent or convey statements that any given system is Year 2000 compliant or that a system will or will not work into the next millennium.

From June through September 1998, using a risk based audit approach, we reviewed and evaluated applicable Year 2000 documentation, including: Treasury's Year 2000 Vulnerability Assessment Report, dated October 1997; the Mint's monthly status reports; the Mint's Year 2000 Project Plan; and other related documents. In addition, we interviewed the appropriate officials within the Mint.

AUDIT RESULTS

Overall, we concluded that the Mint established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. Mint's project management and strategies for conversion, testing, and contingency planning were adequate to address their needs. As a result, no significant reportable issues came to our attention. However, we are making three suggestions which may assist the Mint in sustaining their Year 2000 efforts. Details on the results of our assessment, and our suggestions and Mint's response to these suggestions are provided below.

Project Management

Based on our review, the Mint established an effective Year 2000 project management infrastructure. The Mint identified 28 mission critical IT systems and 19 mission critical non-IT systems. The Mint's ability to become Year 2000 compliant depends on the successful implementation of the Mint's ongoing modernization initiative, Consolidated Information Systems (COINS). COINS will integrate the Mint's ordering, financial, manufacturing, and distribution systems. Accordingly, the Mint's Year 2000 project is divided into: IT for COINS, IT for non-COINS, and non-IT. The non-IT systems are located at the Mint's four manufacturing sites and their bullion depository.

The Mint's Year 2000 project milestones are inextricably linked with the COINS completion dates. As of the September 1998 status report, 16 of the 28 mission critical systems had been either replaced or converted prior to the October 1, 1998 deadline and are awaiting final testing. The remaining 12 systems are scheduled to be fully implemented by the Mint's extended Year 2000 project deadline, December 31, 1998.

System Conversion and Certification Process

The Mint's principle Year 2000 solution is replacing many non-compliant legacy systems with COINS. COINS is a commercial off the shelf based enterprise-wide system development project with some customizations for the Mint's operations. Given the number of internal and external resources associated with this large scale project, coordinating and ensuring Year 2000 compliancy will be especially challenging. To meet this challenge, the Mint pursued several mitigation strategies which include obtaining Year 2000 compliance warranties with their software contractors and requiring independent verification and validation (IV&V) testing for all new systems. The Mint will use outside contractors to conduct IV&V for COINS and related systems; while IV&V for non-COINS will be conducted internally by Mint personnel.

Ensuring Year 2000 Conversion Integrity

The Mint developed processes and procedures to provide for sound change management. The implementation of an enterprise-wide system is sufficiently challenging, only to be compounded by the potential risks posed by the Year 2000. Therefore, sound change management practices are especially critical to apply them to COINS to ensure that the dual objectives of improved operations and Year 2000 compliancy are both met.

It is important for the Mint to ensure that subsequent modifications and environmental changes do not nullify certified test results and their protection under contract warranties. Generally, the risk that a system may fail due to system changes increases as January 1, 2000 approaches and the time available for additional testing decreases. The risk associated with modifying a system will vary depending on the timing and complexity of the changes. The closer system changes occur to the end of testing and certification, the higher the risk. Additionally, the more applications, programs, and interfaces affected by a specific change, the higher the risk to conversion and testing integrity. As organizations complete system, integration, and end to end testing, the likelihood increases that even small changes subsequent to these tests could jeopardize the integrity of certification. Business users and management both have critical roles for managing the risk of system changes. They both need to evaluate potential changes in the context of Year 2000 compliance, and balance the risk to operations of not implementing a change with the risk of rendering a system non-Year 2000 compliant.

One suggested practice to mitigate conversion risk is to adopt "freeze policies," or, as done by the Federal Reserve, put in place a "limitation window and moratorium policy [1]." Whether an organization opts for a complete restriction or limited restriction, it is critical that the timing of such a policy is driven by test schedules and progress. The more

[1] Terms adopted from the Federal Reserve's century date change management policy. The limitation window is the period where there is a higher standard for requesting and approving system changes. A moratorium would occur towards the end of the limitation window, closer to January 1, 2000, and would further restrict changes.

systems that are tested and certified as Year 2000 compliant, or the more aggressive the existing test schedule is, the lower the tolerance should be for approving changes.

Suggestion

1. We suggest that the Mint Director ensures a disciplined change management process is in place to maintain Year 2000 conversion integrity. Once a system has been certified, steps need to be taken to ensure system integrity is maintained. Subsequent changes, including platform upgrades, software enhancements, or any system modification should be evaluated and approved with the understanding of the implications. This could be accomplished by establishing specific criteria for approving system changes. Criteria should address such factors as: nature, timing, and extent of requested change; documented assessment of requested change; extent of retesting required; and number of organizations and partners affected.

   In response to this suggestion, the Mint stated that they recognize the need to manage system growth in a controlled manner. The Mint has established configuration management procedures to ensure future system changes and/or upgrades do not undermine their Year 2000 compliance efforts nor the Mint's operations.

Coordinating Pivot Dates With Data Exchange Partners

We determined that the Mint developed a reasonable plan to address data exchange issues. The Mint identified their external interfaces, and assessed their modification and testing requirements with these data exchange partners. The identification and coordination of internal interfaces is being addressed with the implementation of COINS.

For exchange partners using a windowing logic technique in lieu of a four digit field expansion, special care needs to be given to coordinate pivots.[2] For example, all Treasury bureaus exchange payroll, budget, and accounting data with the National Finance Center and the Financial Management Service, both of which use the windowing logic technique. If exchange partners choose different pivots, the century identifiers could be incorrectly inferred if further processing, calculating, or sorting is performed on data transferred. For example, if the Mint is using a pivot date of 50 and its exchange partner is using a pivot date of 60, date values in between 1950 through 1960 and 2049 through 2059 could be calculated in error. Without coordination with exchange partners, bureaus may not

[2] The windowing logic technique uses pivots to interpret a two digit year into a four digit year. All year values above the pivot are understood to represent one century; while all values below the pivot are understood to represent another century. Pivots refer to a number built into system logic to infer the 2 digit century identifier "19" or "20". For example, a pivot of 50 infers 19 as the century identifier for values 50-99 and infers 20 for values 0-49.

adequately develop and test new data exchange formats, nor apply the necessary bridges and filters to ensure the exchanges will function properly. The greater the number and complexity of data exchanges, the greater the challenge in identifying, synchronizing, and testing exchange formats.

Suggestion

2. We suggest that the Mint Director ensures data exchange procedures include the identification and coordination of pivot dates with its exchange partners. Where there are differences in pivot dates, the Mint should ensure that filters are installed to synchronize and maintain the accuracy of century identifiers. This is especially important between processing partners, i.e., those partners whose data is transferred for further processing.

   In response to this suggestion, the Mint agreed that it should coordinate windowing with its data exchange partners. Written verification will be obtained from its data exchange partners to ensure that all pivot dates and processing logic are in sync. For data exchange with the National Finance Center, a process has been implemented, and all date fields are four character year formats.

Contingency Plans for Business Continuity

The Mint developed limited contingency plans for their mission critical IT systems. These plans consisted of brief action statements included in their monthly status reports, but did not include any detailed business continuity plans. The bulk of the Mint's resources are currently devoted to the development and implementation of COINS. The nature of detailed contingency procedures will be further assessed as COINS implementation nears completion. The risk to continuity of operations will be a function of how many modules are operational and the extent of integration achieved when COINS is implemented. If implementation dates for certain COINS modules slip past December 1998, the Mint is prepared to reinitiate its contingency plan for converting its legacy systems in 1999. With the Year 2000 deadline fast approaching, once past the currently scheduled implementation date, the latitude for further delays decreases, and the need for triggering contingency procedures increases.

Notable efforts by the Mint have been taken to ensure continuity of business with its suppliers and with the Mint's ability to continue manufacturing. First, the Mint hired contractors to perform Year 2000 assessments of the Mint's factories. Second, the contractors assessed the compliance efforts of the Mint's 19 critical suppliers. To date, the Mint's contractors performed site visits to 16 of the suppliers and are scheduled to visit the remaining 3, as well as perform follow-up visits by December 31, 1998. The results from these assessments revealed only minor concerns with their equipment and suppliers.

It is management's responsibility to reduce the risk of Year 2000 related failures and maintain a minimum acceptable level of service. Contingency planning is required to assure continuity of operations in the event of an unanticipated Year 2000 failure, and for systems that will not be Year 2000 compliant. Contingency planning should address risks not only with internal systems, but external risks with business partners and the public infrastructure. Plans should identify resources, procedures, and appropriate training required to carry out core business functions. Plans should clearly identify triggers for implementation, be tested thoroughly, and continuously reevaluated. Steps should be included that facilitate the restoration of normal services at the earliest possible time.

Suggestion

3. We suggest that the Mint Director ensures that management prioritizes and facilitates the preparation and testing of contingency plans for each core business function, as well as mission critical information systems. As part of managing the development and potential implementation of these plans, management should ensure that: these plans consider both the internal and external risks; resources and implementation triggers are identified; training in executing the plan is performed; and the plans are periodically evaluated for reasonableness.

   In response to this suggestion, the Mint stated that continuity of operations plans will be developed and are targeted for completion by March 1999.

We appreciate the courtesies and cooperation provided to our auditors during the audit. If you wish to discuss this report, you may contact me at (202) 622-1090 or a member of your staff may contact Barry L. Savill, Director of Audit at (202) 283-0151.

cc: Treasury Departmental Offices
Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Assistant Director of Information Technology Policy and Management
Director, Office of Organizational Improvement
Director, Office of Strategic Planning
Director, Financial Management Division
Office of Budget
Desk Officer, Management and Controls Branch
Desk Officer, Office of Accounting and Internal

United States Mint
Jay Weinstein, Associate Director for Policy and Management
and Chief Financial Officer
Jackie Fletcher, Chief Information Officer
Cathy Williams, OIG Liaison

Office of Management and Budget
Michael S. Crowley, Budget Examiner

MANAGEMENT RESPONSE

DEPARTMENT OF THE TREASURY
UNITED STATES MINT
WASHINGTON, D.C. 20220

DEC 7 1998

MEMORANDUM FOR DENNIS S. SCHINDEL
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Jay Weinstein
Associate Director/Chief Financial Officer

Jackie Fletcher
Chief Information Officer

SUBJECT: Year 2000 Compliance Effort at the United States Mint (A-DO-98-014)

We appreciate the opportunity to review and comment on your memorandum report regarding the Mint's Year 2000 compliance efforts. The Mint has placed a high priority on making its systems and operations Y2K compliant and is gratified that the OIG determined that we are on target. Although the audit did not identify any areas needing corrective action, the memorandum report contains several suggestions that will help ensure our Y2K effort continues on its successful path.

This review highlighted the significance of ensuring adequate follow-up procedures and controls are in place to assure continued Year 2000 compliance. The Mint recognizes the need to manage system growth in a controlled manner, and has established configuration management procedures to ensure future system changes and/or upgrades do not undermine our Y2K compliance efforts nor Mint operations.

We agree with your observation that the Mint should coordinate windowing with its data exchange partners. The Mint's external interfaces with Mellon Bank and FMS utilize windowing in the exchange of data. Written verification will be obtained from both institutions, to ensure that all pivot dates and processing logic, used in the exchange of data, are in sync. Windowing is not used in the Mint's interface with NFC. Time and attendance is transmitted to NFC via PCTARE, which is a NFC supplied software package, and processed by Pay Period. Pay Period does not contain year as part of the field. During NFC's payroll run a tape is produced, sent back to the Mint, and input into the Labor Distribution System. All date fields on the tape utilize four character year formats.

Your final suggestion emphasizes the importance of detailed contingency plans for each core business function, as well as critical information systems. This suggestion recognizes a valid concern and one the Mint intends to address. Continuity of operations plans will be developed

MANAGEMENT RESPONSE

and are targeted for completion by March, 1999.

As of November 1998, all of our mission critical systems have either been replaced or converted, validated, and implemented into production. COINS went "live" October 1, 1998 in Washington, Philadelphia and West Point. The remaining sites, Denver and San Francisco, went "live" November 1, 1998. These systems will undergo IV&V testing as part of the Certification process. In addition, Year 2000 compliance warranties will be obtained from each vendor who provided the various COTS software that comprises the COINS system.

We would like to acknowledge the work of the audit team on this project; the team kept us informed of their progress, conducted their work in an efficient manner, and was sensitive to the time and informational demands they were placing on us. They are to be commended.

YEAR 2000 COMPLIANCE EFFORT AT THE UNITED STATES MINT

OIG-99-026 **DECEMBER 30, 1998**

Office of Inspector General

****

United States Department of the Treasury